SSOAR

Open Access Repository

www.ssoar.info

Informationsaustausch zwischen Polizei und Nachrichtendiensten strikt begrenzen: Konsequenzen aus dem Urteil des Bundesverfassungsgerichts zur Antiterrordatei

Töpfer, Eric

Veröffentlichungsversion / Published Version
Stellungnahme / comment

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Deutsches Institut für Menschenrechte

Empfohlene Zitierung / Suggested Citation:
Töpfer, E. (2013). *Informationsaustausch zwischen Polizei und Nachrichtendiensten strikt begrenzen: Konsequenzen aus dem Urteil des Bundesverfassungsgerichts zur Antiterrordatei.* (Policy Paper / Deutsches Institut für Menschenrechte, 21). Berlin: Deutsches Institut für Menschenrechte. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-349315

Nutzungsbedingungen:
Dieser Text wird unter einer Deposit-Lizenz (Keine Weiterverbreitung - keine Bearbeitung) zur Verfügung gestellt. Gewährt wird ein nicht exklusives, nicht übertragbares, persönliches und beschränktes Recht auf Nutzung dieses Dokuments. Dieses Dokument ist ausschließlich für den persönlichen, nicht-kommerziellen Gebrauch bestimmt. Auf sämtlichen Kopien dieses Dokuments müssen alle Urheberrechtshinweise und sonstigen Hinweise auf gesetzlichen Schutz beibehalten werden. Sie dürfen dieses Dokument nicht in irgendeiner Weise abändern, noch dürfen Sie dieses Dokument für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, aufführen, vertreiben oder anderweitig nutzen.
Mit der Verwendung dieses Dokuments erkennen Sie die Nutzungsbedingungen an.

Terms of use:
This document is made available under Deposit Licence (No Redistribution - no modifications). We grant a non-exclusive, non-transferable, individual and limited right to using this document. This document is solely intended for your personal, non-commercial use. All of the copies of this documents must retain all copyright information and other information regarding legal protection. You are not allowed to alter this document in any way, to copy it for public or commercial purposes, to exhibit the document in public, to perform, distribute or otherwise use the document in public.
By using this particular document, you accept the above-stated conditions of use.

gesis Leibniz-Institut für Sozialwissenschaften

Mitglied der Leibniz-Gemeinschaft

Policy Paper

Informationsaustausch zwischen Polizei und Nachrichtendiensten strikt begrenzen

Konsequenzen aus dem Urteil des Bundesverfassungsgerichts zur Antiterrordatei

Eric Töpfer

Deutsches Institut
für Menschenrechte

Impressum

Deutsches Institut für Menschenrechte

Zimmerstr. 26/27
10969 Berlin
Tel.: 030 25 93 59 - 0
Fax: 030 25 93 59 - 59
info@institut-fuer-menschenrechte.de
www.institut-fuer-menschenrechte.de

Satz:
Wertewerk
Barrierefreies Publizieren
Tübingen

Policy Paper Nr. 21
Juni 2013

ISBN 978-3-942315-71-5 (PDF)
ISSN 1614-2195 (PDF)

© 2013 Deutsches Institut für Menschenrechte
Alle Rechte vorbehalten

Der Autor

Eric Töpfer ist wissenschaftlicher Mitarbeiter am Deutschen Institut für Menschenrechte. Sein Arbeitsschwerpunkt ist der Menschenrechtsschutz im Politikfeld Innere Sicherheit. Außerdem ist er für die sozialwissenschaftliche Berichterstattung an die Agentur der Europäischen Union für Grundrechte zuständig.

Das Institut

Das **Deutsche Institut für Menschenrechte** ist die unabhängige Nationale Menschenrechtsinstitution Deutschlands. Es ist gemäß den Pariser Prinzipien der Vereinten Nationen akkreditiert (A-Status). Zu den Aufgaben des Instituts gehören Politikberatung, Menschenrechtsbildung, Information und Dokumentation, angewandte Forschung zu menschenrechtlichen Themen sowie die Zusammenarbeit mit nationalen und internationalen Organisationen. Es wird vom Bundesministerium der Justiz, vom Auswärtigen Amt und von den Bundesministerien für wirtschaftliche Zusammenarbeit und Entwicklung sowie für Arbeit und Soziales gefördert. Im Mai 2009 wurde die Monitoring-Stelle zur UN-Behindertenrechtskonvention im Institut eingerichtet.

Inhalt

Informationsaustausch zwischen Polizei und Nachrichtendiensten strikt begrenzen

Konsequenzen aus dem Urteil des Bundesverfassungsgerichts zur Antiterrordatei

1 Einleitung

Sechs Jahre nach Inbetriebnahme der Antiterrordatei (ATD) hat das Bundesverfassungsgericht über die Verfassungsbeschwerde eines pensionierten Richters gegen das Gesetz zur Errichtung der Datei entschieden. Am 24. April 2013 erklärte der Erste Senat die gemeinsame Verbunddatei von Polizei und Nachrichtendiensten in ihren „Grundstrukturen" für verfassungskonform, stellte aber gleichzeitig einzelne Vorschriften des Gesetzes als verfassungswidrig fest. Nun muss der Gesetzgeber das Antiterrordateigesetz (ATDG) bis Ende 2014 entsprechend überarbeiten.

In dem Verfahren war das Deutsche Institut für Menschenrechte vom Bundesverfassungsgericht zur Stellungnahme in der mündlichen Verhandlung am 6. November 2012 eingeladen worden, nachdem es im März 2012 grundsätzliche Bedenken gegen die Einrichtung der am Vorbild ATD orientierten Rechtsextremismusdatei (RED) vorgebracht hatte.[1] Mit dem vorliegenden Policy Paper informiert das Institut über die Datei und das Urteil. Dabei stellt es die Entscheidung des Gerichts in den Kontext der Diskussionen über eine engere Zusammenarbeit der Sicherheitsbehörden, die mit der Aufarbeitung der rechtsterroristischen Morde des „Nationalsozialistischen Untergrunds" neuen Auftrieb erhalten haben. Das Policy Paper formuliert erste Empfehlungen an die Gesetzgeber in Bund und Ländern zur grund- und menschenrechtlich gebotenen Begrenzung und Kontrolle des Informationsaustausches zwischen der Polizei und den Nachrichtendiensten.

2 Zur Entstehung des Gesetzes

Das Antiterrordateigesetz geht auf einen Vorstoß der Ständigen Konferenz der Innenminister und senatoren (IMK) zurück, die sich unter dem Eindruck der Madrider Anschläge vom 11. März 2004 im Juli des Jahres auf ihrer 174. Sitzung für die „Errichtung gemeinsamer Dateien, insbesondere einer Aktenfundstellendatei, für Vorgänge der Verfassungsschutzbehörden und Polizeien von Bund und Ländern und gegebenenfalls weiteren Sicherheitsbehörden des Bundes über Personen und Vorgänge aus dem Bereich des islamistischen Terrorismus einschließlich des islamistischen Extremismus" aussprachen und die Prüfung der Möglichkeiten in Auftrag gaben.[2] Noch bevor die anschließend installierte Arbeitsgruppe des Bundesministerium des Innern (BMI) unter Einbeziehung der beiden IMK-Arbeitskreise II (Innere Sicherheit) und IV (Verfassungsschutz) am 10. November 2004 ihren abschließenden Bericht zu den Optionen vorgelegt hatte, brachten am 1. September die Länder Niedersachsen, Bayern, Saarland und Thüringen einen ersten Entwurf für ein Gesetz „zur Errichtung einer gemeinsamen Datei der deutschen Sicherheitsbehörden zur Beobachtung und Bekämpfung des islamistischen Extremismus und Terrorismus" (Anti-Terror-Datei-Gesetz) in den Bundesrat ein.[3] Der Entwurf, der die Errichtung einer umfassenden gemeinsamen Volltextdatei von Kriminalämtern und Geheimdiensten beim Bundesamt für Verfassungsschutz vorsah, wurde am 15. Oktober des Jahres mit den Stimmen der Unions-geführten Länder vom Bundesrat beschlossen. Letztlich scheiterte der Entwurf allerdings

1 S. Drohla, Jeannine (2012): Schriftliche Stellungnahme zur öffentlichen Anhörung zum Entwurf eines Gesetzes zur Verbesserung der Bekämpfung des Rechtsextremismus (BT-Drucksache 17/8672) am 19.03.2012. Berlin: Deutsches Institut für Menschenrechte. https://www.bundestag.de/bundestag/ausschuesse17/a04/Anhoerungen/Anhoerung17/Stellungnahmen_weitere/Stellungnahme_01.pdf [abgerufen am 1. Juni 2013]. Nachdem das Gesetz Ende August 2012 in Kraft getreten war, ging die Rechtsextremismusdatei am 19. September 2012 in Betrieb.

2 Ständige Konferenz der Innenminister und -senatoren der Länder: Sammlung der zur Veröffentlichung freigegebenen Beschlüsse der 174. Sitzung der Ständigen Konferenz der Innenminister und -senatoren am 8. Juli 2004 in Kiel, S. 2-5.

3 Bundesrat: Drucksache 657/04 vom 01.09.2004.

im Bundestag, wo er am 30. Juni 2005 auf Empfehlung des Innenausschusses gegen die Stimmen der Union abgelehnt wurde.

Ein zweiter Vorstoß für ein Gesetz zur Schaffung einer Antiterrordatei folgte im Herbst 2006 mit dem Entwurf der nunmehr schwarz-roten Bundesregierung für ein „Gesetz für die Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder" (Gemeinsame-Dateien-Gesetz, GDG),[4] das als Artikelgesetz die Errichtung einer zentralisierten, standardisierten Antiterrordatei vorsah (Art. 1) sowie zur Regelung der Errichtung gemeinsamer Projektdateien eine Änderung der Gesetze über das Bundeskriminalamt (BKA) und den Bundesnachrichtendienst (BND) und des Bundesverfassungsschutzgesetzes (Art. 2-4). Der Entwurf wurde dem Bundesrat am 22. September als „besonders eilbedürftig", aber „nicht zustimmungspflichtig" zugeleitet, ging am 16. Oktober an den Bundestag und wurde knapp zwei Monate später – am 22. Dezember 2006 – mit den Stimmen der Großen Koalition verabschiedet. In der die Abstimmung vorbereitenden Sitzung des Innenausschusses wurde ein Alternativentwurf der Fraktion Bündnis 90/Die Grünen zur Schaffung einer reinen Indexdatei ebenso abgelehnt wie ein Antrag der Linksfraktion, auf die Schaffung einer ATD gänzlich zu verzichten.[5] Gegenüber dem ursprünglichen Entwurf wurden kleine Änderungen vorgenommen, unter anderem schränkte man den Kreis der zu speichernden Kontaktpersonen auf „nicht nur flüchtig oder in zufälligem Kontakt" mit Verdächtigen in Verbindung stehende Personen ein, ergänzte einen § 13 zur Einschränkung von Grundrechten (Brief-, Post- und Fernmeldegeheimnis sowie der Unverletzlichkeit der Wohnung) und verlängerte die ursprünglich für sechs Jahre gedachte Befristung des GDG auf elf Jahre.[6] Das Ansinnen des Bundesrates, an der geplanten Evaluierung beteiligt zu werden, wies die Bundesregierung zurück. Das Gesetz trat am 31. Dezember 2006 in Kraft.[7] Am 30. März 2007 ging die Antiterrordatei in Betrieb.

3 Die Datei im Kontext „vernetzter Sicherheit"

Seit Inbetriebnahme der ATD wurden wiederholt Forderungen laut, die Recherchemöglichkeiten der Datei auszubauen und sie mit Auswerte- und Analysefunktionen zu versehen. Zuletzt berichtete die Bundesregierung in ihrer Evaluierung des Antiterrordateigesetzes von Wünschen der Nutzerinnen und Nutzer nach einer funktionalen Weiterentwicklung, „um bereits innerhalb der Verbunddatei weiterführende Erkenntnisse zu gewinnen und den Informationsaustausch noch besser strukturieren zu können".[8] Gefordert wird zum Beispiel die Möglichkeit, direkt in der ATD Zusammenhänge zwischen Personen, Gruppierungen und Objekten herzustellen. In ähnlichem Tenor erklärte die IMK auf ihrer Herbstsitzung 2012 in ihrem Beschluss zur Eröffnung des neuen Gemeinsamen Extremismus- und Terrorismusabwehrzentrum (GETZ): „Die IMK hält unter Berücksichtigung der bevorstehenden Entscheidung des Bundesverfassungsgerichts zur ATD Dateien für alle Phänomenbereiche des gewaltorientierten Extremismus, die auch umfassende Analyse- und Recherchemöglichkeiten eröffnen, für erforderlich."[9]

Die ATD steht damit stellvertretend für die wachsende informationelle Zusammenarbeit zwischen Polizei und Nachrichtendiensten, die im Zeichen des neuen Paradigmas der „vernetzten Sicherheit" seit dem 11. September 2001 vorangetrieben wird. Neu ist die informationelle Zusammenarbeit allerdings nicht. So regelten bereits die geheim gehaltenen Unkeler Richtlinien vom 8. Oktober 1954 die Zusammenarbeit zwischen Verfassungsschutz, BND, Militärischem Abschirmdienst (MAD) und dem polizeilichen Staatsschutz, und bis in die frühen 1990er Jahre bestand ein elektronischer Indexzugriff des BKA auf das Nachrichtendienstliche Informationssystem (NADIS) der Verfassungsschutzbehörden und umgekehrt des Verfassungsschutzes auf die „Arbeitsdatei PIOS Innere Sicherheit" des BKA.[10] Gekappt wurde diese erst im Kontext der Diskussionen um die Notwendigkeit einer rechtlichen Normierung der geheimdienstlichen Datenverarbeitung im Gefolge

4 Deutscher Bundestag: Drucksache 16/2950 vom 16.10.2006.
5 Deutscher Bundestag: Drucksache 16/3642 vom 29.11.2006.
6 Deutscher Bundestag: Drucksache 16/3642 vom 29.11.2006.
7 BGBl. 2006: Teil I, S. 3409.
8 Deutscher Bundestag: Drucksache 17/12665 vom 07.03.2013, S. 5.
9 Ständige Konferenz der Innenminister und -senatoren der Länder: Sammlung der zur Veröffentlichung freigegebenen Beschlüsse der 196. Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder vom 05.12. – 07.12.2012 in Rostock-Warnemünde, S. 37.
10 Vgl. zum Beispiel Gusy, Christoph (1982): Das nachrichtendienstliche Informationssystem (NADIS). In: Datenverarbeitung im Recht. Band 11, S. 251–266.

des Volkszählungsurteils des Bundesverfassungsgerichts, deren Ergebnis das „Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes" vom 20. Dezember 1990 war,[11] das unter anderem erstmals die Arbeit von BND und MAD auf eine gesetzliche Grundlage stellte. Bereits damals notierte der Leiter der Staatsschutzabteilung des BKA: „Aus meiner Sicht wäre es zweckmäßig, einen automatisierten Informationsaustausch zwischen Bundeskriminalamt und Bundesamt für Verfassungsschutz zu installieren. Neben der Beschleunigung des Informationsaustauschs und dem Nachweis der Unterrichtung aus dem System heraus entstünde eine vordefinierbare Informationsgestellung, die spezifische Interessen der Landesverrats-, der Extremismus- und der Terrorismusbekämpfung sowie der Bekämpfung der politisch motivierten Ausländerkriminalität umfassen könnte."[12]

Zur gleichen Zeit begann mit der Einrichtung der „Koordinierungsgruppe Terrorismusbekämpfung" (1991) und der „Informationsgruppe zur Beobachtung und Bekämpfung rechtsextremistischer/-terroristischer, insbesondere fremdenfeindlicher Gewaltakte" (1992) eine institutionalisierte Kooperation von Verfassungsschutz, Kriminalämtern und Generalbundesanwaltschaft in hybriden Strukturen,[13] in deren Tradition die gemeinsamen Zentren stehen, die nach dem 11. September 2001 installiert wurden. Namentlich handelt es sich dabei um:

- das **Gemeinsame Terrorismusabwehrzentrum (GTAZ)** in Berlin-Treptow
- das **Gemeinsame Analyse- und Strategiezentrum illegale Migration (GASiM)** in Potsdam
- das **Gemeinsame Internetzentrum (GIZ)** in Berlin-Treptow
- das **Nationale Cyberabwehrzentrum (NCAZ)** in Bonn
- das **Gemeinsame Extremismus- und Terrorismusabwehrzentrum (GETZ)** an den beiden Standorten Köln und Meckenheim, in welches das als Konsequenz aus der Mordserie des NSU gegründete **Gemeinsame Abwehrzentrum gegen Rechtsextremismus (GER)** überführt wurde.

Legende zur Tabelle 1, Seite 7

BKA	=	Bundeskriminalamt
BPol	=	Bundespolizei
GBA	=	Generalbundesanwalt
ZKA	=	Zollkriminalamt
BSI	=	Bundesamt für Sicherheit in der Informationstechnik
BBK	=	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BAMF	=	Bundesamt für Migration und Flüchtlinge
BAFA	=	Bundesamt für Wirtschaft und Ausfuhrkontrollen
AA	=	Auswärtiges Amt
BfV	=	Bundesamt für Verfassungsschutz
BND	=	Bundesnachrichtendienst
MAD	=	Militärischer Abschirmdienst
LKÄ	=	Landeskriminalämter
LfV	=	Landesbehörden für Verfassungsschutz

11 BGBl. 1990: Teil I, S. 2954.

12 Walter, Dieter (1991): Notwendigkeit der Zusammenarbeit zwischen polizeilichem Staatsschutz und Verfassungsschutz aus der Sicht des Bundeskriminalamtes. In: Hans-Ludwig Zachert (Hg.): 40 Jahre Bundeskriminalamt, Stuttgart u.a.: Boorberg, S. 232.

13 Vgl. Wörlein, Jan (2008): Unkontrollierbare Anziehungskraft. Institutionalisierte Kooperation von Polizei und Diensten. In: Bürgerrechte & Polizei/CILIP, Heft 90 (2/2008), S. 50-61.

Tabelle 1: Die Gemeinsamen Zentren

	GTAZ	GASIM	GIZ	NCAZ	GETZ/GER
Zweck	Zusammenarbeit der Sicherheitsbehörden zur Bekämpfung des islamistischen Terrorismus	Intensivierung der Zusammenarbeit bei der Bekämpfung der illegalen Migration und ihrer Begleit- und Folgekriminalität	Sichtung, Auswertung und Analyse islamistischer und jihadistischer Internetinhalte mit Deutschlandbezug sowie die behördenübergreifende Berichterstattung	Optimierung der operativen Zusammenarbeit relevanter staatlichen Stellen und Koordinierung der Schutz- und Abwehrmaßnahmen gegen IT-Vorfälle	Bündelung der Kooperation zwischen den Sicherheitsbehörden zu den Phänomenbereichen Rechtsextremismus/-terrorismus, Linksextremismus/-terrorismus, Ausländerextremismus/-terrorismus, Spionageabwehr und Proliferation
Einrichtung	14. Dezember 2004	17. Juli 2006 (Vorläufer Gemeinsames Analyse- und Strategiezentrum Schleusungskriminalität bereits im November 2004)	2. Januar 2007	1. April 2011	15. November 2012 [14] (GER seit 16. Dezember 2011)
Mitarbeitende	229, davon 198 Bund und 31 Länder (Stand 2008) [15]	18 Personen (Stand: 2011) [16] – gegenüber 40 Personen in 2007 [17]	51 (Stand: 2011 – 2007 mit 15 Mitarbeitenden eingerichtet) [18]	10 Personen aus den ständig im NCAZ vertretenen „Kernbehörden" (Stand 2011) [19]	130-140, davon 50 vom BKA und 50 vom BfV (Stand Dezember 2011 bei Einrichtung des GER) [20]
Zahl beteiligter Behörden	40	5 Kernbehörden 2 assoziierte Behörden	5	3 Kernbehörden 5 assoziierte Behörden	42
Geschäftsführung/ Federführung	Gemeinsame Geschäftsführung	Bundespolizeipräsidium	BfV	BSI	Gemeinsame Geschäftsführung durch BfV und BKA
Standort	Berlin-Treptow	Potsdam	Berlin-Treptow	Bonn	Köln (BfV) / Meckenheim (BKA Abteilung ST)
BKA	X	2 Personen	X	anlassbezogen	X
BPol	X	9 Personen		anlassbezogen	X
GBA	X		X		X
ZKA	X			anlassbezogen	X
Finanzkontrolle Schwarzarbeit		1 Person			
BSI				6 Personen	
BBK				2 Personen	
BAMF	X	5 Personen			X
BAFA					X
AA		anlassbezogen			
Bundeswehr				anlassbezogen	
BfV	X	anlassbezogen	X	2 Personen	X
BND	X	1 Person	X	anlassbezogen	X
MAD	X		X		X
16 LKÄ	X				X
16 LfV	X				X
Europol					X

14 Bundesamt für Verfassungsschutz (ohne Datum): Presseinformationen zum Start des Gemeinsamen Extremismus- und Terrorismusabwehrzentrums. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/Extremismus/getz.pdf?__blob=publicationFile [abgerufen am 25. Mai 2013].
15 Deutscher Bundestag: Drucksache 16/10007 vom 18.07.2008.
16 Deutscher Bundestag: Drucksache 17/6720 vom 02.08.2011.
17 Deutscher Bundestag: Drucksache 16/8482 vom 11.03.2008.
18 Deutscher Bundestag: Drucksache 17/5695 vom 02.05.2011.
19 Deutscher Bundestag: Drucksache 17/5694 vom 02.05.2011.
20 Bundesministerium des Innern (ohne Datum): Gemeinsames Abwehrzentrum gegen Rechtsextremismus. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Kurzmeldungen/gar_handout.pdf;jsessionid=D9B36C24726F4435F3336B832D5E9F69.2_cid295?__blob=publicationFile [abgerufen am 25. Mai 2013].

Diskutiert wird gegenwärtig die Zusammenführung der beiden größten Zentren GTAZ und GETZ zu einem „phänomenübergreifenden Zentrum". Während eine solche Lösung von der großen Mehrheit der Länder insbesondere aus Gründen der Ressourcenschonung befürwortet wird, stößt sie bislang beim BMI auf Widerstände.[21] Käme sie zustande, würden künftig vermutlich mehr als 400 Mitarbeitende verschiedener Sicherheitsbehörden aus Bund und Ländern unter einem Dach in Berlin-Treptow zusammenarbeiten.

Auch wenn der Kreis der teilnehmenden Behörden deutlich variiert und Sicherheitsfachleute ihren Nutzen im Einzelnen unterschiedlich bewerten,[22] ist allen gemeinsamen Zentren gemeinsam, dass sie als „Informationsdrehscheiben" Mitarbeitende sowohl aus Polizeibehörden als auch Geheimdiensten regelmäßig in übergreifenden Plenen und thematischen Arbeitsgruppen zusammenbringen, um umfassende Lagebilder und Gefahrenanalysen zu erstellen und operative Maßnahmen abzustimmen. Kritik, dass mit den Zentren eine gebotene Trennung von Polizei und Diensten unterlaufen würde, weist das BMI regelmäßig mit der Begründung zurück, dass es sich trotz der auf Dauer angelegten Zusammenarbeit nicht um neue Behörden handele, sondern die Beteiligten auf Grundlage ihrer jeweils eigenen gesetzlichen Aufträge und Befugnisse zusammenarbeiten.

Recht deutlich wird allerdings der Abschlussbericht der vierköpfigen Bund-Länder-Kommission Rechtsterrorismus (BLKR). In ihrer Analyse zu den Gründen für das Versagen der Sicherheitsbehörden angesichts der Morde und Überfälle des „Nationalsozialistischen Untergrundes" (NSU) bilanziert sie – ohne allerdings ernsthaft der Frage nachzugehen, warum die Ermittlungen nahezu ausschließlich in eine Richtung geführt wurden – ein „Trennungsgebot in den Köpfen" als ursächlich für die Probleme in der Zusammenarbeit zwischen Verfassungsschutz- und Polizeibehörden: „Diese ‚Kopfsperre' muss bei Polizei und Verfassungsschutz zu Gunsten eines gemeinsamen Verständnisses von Verantwortung für die Sicherheit abgebaut werden."[23] Hierzu empfiehlt die Kommission unter anderem eine Harmonisierung der gesetzlichen Übermittlungsvorschriften. Dadurch soll sichergestellt werden, dass „Schnittstellenprobleme, unterschiedliche fachliche Standards, mangelnde Kenntnisse der Arbeitsweise des jeweiligen Gegenübers bestmöglich überwunden bzw. kompensiert werden können". Für die Übermittlung von Erkenntnissen regt sie die Entwicklung eines standardisierten Verfahrens für eine strukturierte Informationsübermittlung an.[24] Im Zeichen solcher Empfehlungen erscheint es denkbar, dass zumindest mittelfristig – analog zu den Überlegungen zur Fusion von GTAZ und GETZ – auch eine Zusammenführung der beiden bestehenden Verbunddateien ATD und RED und ihre Ausweitung auf andere Phänomenbereiche angestrebt werden könnte.

4 Gesetz und Datei im Überblick

Nach § 1 Abs. 1 ATDG ist die Antiterrordatei eine „standardisierte zentrale" Datei, die gemeinsam vom Bundeskriminalamt (BKA), dem Bundespolizeipräsidium, den Landeskriminalämtern (LKÄ), den Verfassungsschutzbehörden von Bund und Ländern, Militärischem Abschirmdienst (MAD), Bundesnachrichtendienst (BND) und Zollkriminalamt (ZKA) beim BKA geführt wird. Zweck der Datei ist die Erfüllung der jeweiligen gesetzlichen Aufgaben zur „[geheimdienstlichen][25] Aufklärung oder [polizeilichen] Bekämpfung des internationalen Terrorismus mit Bezug zur Bundesrepublik Deutschland". Im Gegensatz zu den ursprünglichen Plänen ist die Datei nicht ausschließlich auf den islamistischen Terrorismus beschränkt, sondern bezieht sich auch auf andere Bereiche des internationalen Terrorismus, sofern ein hinreichender Bezug zu Deutschland vorliegt. Dies kann zum Beispiel auch säkulare Gruppen wie die kurdische PKK oder die Volksmodjahedin Iran (MEK) betreffen.[26] Entsprechend § 1 Abs. 2 ATDG können weitere Polizeivollzugsbehörden zur Teilnahme berechtigt werden, wenn sie nicht nur im Einzelfall mit der Terrorismusbekämpfung beschäftigt sind; Einzelheiten regelt nach § 12 ATDG die Errich-

21 Ständige Konferenz der Innenminister und -senatoren der Länder: Sammlung der zur Veröffentlichung freigegebenen Beschlüsse der 196. Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder vom 05.12. – 07.12.2012 in Rostock-Warnemünde, S. 36ff.

22 Vgl. die Einschätzung der Werthebach-Kommission zu GTAZ und GASiM. Kommission „Evaluierung Sicherheitsbehörden" (2010): Kooperative Sicherheit. Die Sonderpolizeien des Bundes im föderalen Staat. Bericht und Empfehlungen der Kommission „Evaluierung Sicherheitsbehörden" vom 09.12.2010, S. 124ff.

23 Bundesministerium des Innern und Ständige Konferenz der Innenminister und –senatoren der Länder (Hg.) (2013): Abschlussbericht der Bund-Länder-Kommission Rechtsterrorismus. Zusammenfassung der Empfehlungen vom 30.04.2013, S. 3.

24 Ebda., S. 6f.

25 Einfügungen in eckigen Klammern vom Autor.

26 Vgl. Bundesministerium des Innern: Bericht „Möglichkeiten zur Schaffung von gemeinsamen Dateien von Polizei und Nachrichtendiensten im Bereich der Terrorismusbekämpfung" vom 10.11.2004, S. 8.

tungsanordnung, die mit Stand vom 4. Juni 2010 insgesamt 23 lokale Polizeidienststellen aus Baden-Württemberg, Bayern und Rheinland-Pfalz als weitere beteiligte Behörden auflistet.

Nach dem Muster der seit den 1970er Jahren existierenden PIOS-Dateien verpflichtet das Antiterrordateigesetz die an der ATD beteiligten Behörden zur Speicherung bereits erhobener Daten zu Personen, Institutionen, Objekten und Sachen, erstens, im Zusammenhang mit „terroristischen Vereinigungen" nach § 129a Strafgesetzbuch (StGB), die einen internationalen Bezug aufweisen, zweitens, im Zusammenhang mit „terroristischen Vereinigungen im Ausland" nach § StGB 129a in Verbindung mit § 129b Abs. 1 Satz 1 StGB , die einen mit Bezug zur Bundesrepublik Deutschland haben, oder, drittens, im Zusammenhang mit „rechtswidrig[er] Gewalt als Mittel zur Durchsetzung international ausgerichteter politischer oder religiöser Belange" (§ 2 Satz 1 Nr. 2 ATDG). Gespeichert werden sollen Daten zu Personen, gegen die Erkenntnisse vorliegen, aus denen sich „tatsächliche Anhaltspunkte" ergeben, dass diese einer entsprechenden terroristischen Vereinigung angehören, sie unterstützen oder Unterstützer von Unterstützern sind (§ 2 Satz 1 Nr. 1 ATDG). Unter den gleichen Voraussetzungen sind außerdem Daten zu Personen zu speichern, über die Erkenntnisse vorliegen, dass sie eben genannte „rechtswidrige Gewalt" anwenden, unterstützen, vorbereiten, befürworten oder „durch ihre Tätigkeiten vorsätzlich hervorrufen" (§ 2 Satz 1 Nr. 2 ATDG). Darüber hinaus sollen Personen, die mit den zuvor genannten „nicht nur in flüchtigen oder zufälligem Kontakt" stehen und von denen „weiterführende Hinweise für die Aufklärung oder Bekämpfung des internationalen Terrorismus zu erwarten sind" als Kontaktpersonen in der Datei erfasst werden (§ 2 Satz 1 Nr. 3 ATDG). Nicht zuletzt sind – außer für Kontaktpersonen – Vereinigungen, Gruppierungen, Stiftungen und Unternehmen sowie Sachen, Bankverbindungen, Anschriften, Telekommunikationsanschlüsse und -geräte sowie Internetseiten und Email-Adressen zu speichern, die im Zusammenhang mit den genannten Personen stehen (§ 2 Satz 1 Nr. 4 ATDG).

Während für die Institutionen, Objekte und Sachen grundsätzlich „Angaben zur Identifizierung" gespeichert werden (§ 3 Abs. 2 ATDG), werden zu Personen, je nach Personenkategorie, unterschiedlich viele Informationen gespeichert. Für alle oben genannten Kategorien von Personen werden sogenannte Grunddaten gespeichert (§ 3 Abs. 1 Nr. 1a ATDG): Namen, Aliaspersonalien, Geschlecht, Geburtsdatum, -ort, -staat, (ehemalige) Staatsangehörigkeiten, (ehemalige) Anschriften, besondere körperliche Merkmale, Sprachen und Dialekte, Lichtbilder (Fotos und Fingerabdrücke) und in der Regel Angaben zu Identitätspapieren. Hingegen sind für mutmaßliche oder tatsächliche Terroristen und ihre direkten und indirekten Unterstützer sowie für all jene, die mutmaßlich oder tatsächlich „rechtswidrig Gewalt als Mittel zur Durchsetzung international ausgerichteter politischer oder religiöser Belange" anwenden, unterstützen, vorbereiten, befürworten oder vorsätzlich hervorrufen sowie für sogenannte dolose Kontaktpersonen, die verdächtigt werden, von der Planung und Begehung terroristischer Straftaten oder der Ausübung, Unterstützung oder Vorbereitung „rechtswidriger Gewalt" Kenntnis zu haben, auch erweiterte Grunddaten zu speichern (§ 3 Abs. 1 Nr. 1b ATDG): Das sind eigene oder genutzte Telekommunikationsanschlüsse und -endgeräte, Emailadressen, Bankverbindungen, Schließfächer, eigene oder genutzte Fahrzeuge, Familienstand, Volkszugehörigkeit, Angaben zur Religionszugehörigkeit „soweit diese im Einzelfall [...] erforderlich sind", besondere Fähigkeiten mit Relevanz für die Begehung „terroristischer Straftaten", Angaben zu Schulabschluss, Berufsausbildung und ausgeübtem Beruf, Angaben zu (ehemaligen) Tätigkeiten in lebenswichtigen Einrichtungen, Angaben zur Gefährlichkeit, Fahr- und Flugerlaubnisse, besuchte Treffpunkte (Orte oder Gebiete), Kontaktpersonen, Namen von Vereinigungen oder Gruppierungen sowie „zusammenfassende besondere Bemerkungen, ergänzende Hinweise und Bewertungen". Mit Ausnahme dieses letzten in der technischen Umsetzung auf 2.000 Zeichen beschränkten Freitextfeldes [27] handelt es sich bei allen anderen zu speichernden Angaben um standardisierte Daten, die eine schnelle Durchsuchbarkeit und den automatisierten Abgleich mit anderen Datenbeständen ermöglichen. Zu allen Daten sind außerdem die zugehörigen Aktenzeichen oder sonstige Geschäftszeichen zu speichern.

Zum Schutz von behördlichen Geheimhaltungsinteressen oder besonders schutzwürdigen Interessen von Betroffenen können die erweiterten Grunddaten zu Personen entweder beschränkt oder verdeckt gespeichert werden (§ 4 ATDG). Eine beschränkte Speicherung bedeutet, dass die Daten entgegen der grundsätzlichen Speicherungspflicht gar nicht oder nur teilweise gespeichert werden. Eine verdeckte Speicherung meint, dass im Falle einer Abfrage durch eine andere beteiligte Behörde diese keine Treffermeldung erhält, son-

27 BVerfG: Urteil vom 24.04.2013, Aktenzeichen 1 BvR 1215/07, Randnummer (Rn.) 69.

dern nur die einstellende Behörde informiert wird, um unverzüglich Kontakt aufzunehmen und zu klären, ob ein Informationsaustausch geboten ist.

Konzipiert ist die ATD als Kombination aus Volltext- und Indexdatei. Nach § 5 ATDG können die beteiligten Behörden die Datei im „automatisierten Verfahren" nutzen. Im Falle eines Treffers, also bei einer Übereinstimmung eines Suchdatums (zum Beispiel Name, Adresse oder Telefonnummer eines Verdächtigen) mit dem abgefragten Datenbestand, erhält die abfragende Stelle Zugriff auf die zu Personen gespeicherten „Grunddaten" beziehungsweise auf die Angaben zu Institutionen, Objekten und Sachen im Volltext (§ 5 Abs 1 Nr. 1). Auf die zu Personen gespeicherten „erweiterten Grunddaten" erhält die abfragende Stelle hingegen keinen Volltextzugriff, sondern nur die Mitteilung, dass ein Treffer vorliegt, sowie Angaben zur Stelle, die die Daten eingegeben hat (Indexfunktion). Durchsucht werden kann dabei nicht nur der Bestand an einfachen Grunddaten, sondern der gesamte Datenbestand, so dass gewissermaßen „blind" zum Beispiel mit einem Namen im nicht unmittelbar einsehbaren Bestand erweiterter Grunddaten nach Hauptpersonen gesucht werden kann, denen die namentlich bekannte Person als Kontakt zugeordnet ist. Technisch möglich ist auch die Suche nach Telefon- und Kontonummern oder Treffpunkten, die alle hiermit in Zusammenhang gebrachten Personen als „Treffer" auswerfen würde. Begrenzt ist die Anzeige der Ergebnisse einer solchen „Inverssuche" nach Angaben der Bundesregierung auf 200 Treffer.[28]

Im Falle eines Treffers kann die dateneingebende Stelle angefragt werden, ob sie den Zugriff auf die erweiterten Grunddaten im konkreten Einzelfall im Rahmen der jeweils geltenden Übermittlungsvorschriften freigibt (§ 5 Abs 1 Nr. 1 ATDG). Ausnahmen von dieser Regel sind nur für den „Eilfall" vorgesehen (§ 5 Abs. 2 ATDG): „[Z]ur Abwehr einer gegenwärtigen Gefahr für Leib, Leben, Gesundheit oder Freiheit einer Person oder für Sachen von erheblichem Wert, deren Erhaltung im öffentlichen Interesse geboten ist", können die Leiter der beteiligten Behörden oder stellvertretend von diesen bestimmte Beamte des höheren Dienstes, also zum Beispiel Referatsleiter, entscheiden, dass unmittelbar auf die erweiterten Grunddaten zugegriffen wird, diese also ohne Anfrage bei der dateneingebenden Stelle im Volltext ausgelesen werden. Eilfall-Entscheidungen und ihre Begründung sind zu dokumentieren und der Zugriff ist technisch zu protokolieren. Die nachträgliche Zustimmung der dateneingebenden Stelle ist „unverzüglich" einzuholen. Wird sie verweigert, ist die weitere Verwendung der Daten unzulässig; die Daten sind zu löschen oder zu sperren. Aber auch für Standardabfragen der ATD sind der Zweck und die Dringlichkeit anzugeben und zu protokollieren (§ 5 Abs. 4 ATDG).

Nach §§ 6 und 7 ATDG darf eine abfragende Behörde die Daten, auf die sie Zugriff erhalten hat, nur nutzen, um zu prüfen, ob der Treffer der gesuchten Person, Institution oder Sache zuzuordnen ist, und um anschließend bei der einstellenden Behörde auf Grundlage des einschlägigen Fachrechts um die Übermittlung weiterer Informationen zu ersuchen. Eine Verwendung der Trefferdaten zu anderen Zwecken als der Aufklärung und Bekämpfung des internationalen Terrorismus ist nicht ausgeschlossen. Zulässig ist sie, wenn dies „zur Verfolgung einer besonders schweren Straftat oder zur Abwehr einer Gefahr für Leib, Leben, Gesundheit oder Freiheit einer Person erforderlich ist" und die dateneingebende Behörde dieser Verwendung zugestimmt hat. In einem solchen Fall sind die Daten zu kennzeichnen, um ihre Übernahme aus der ATD zu markieren.

Datenschutzrechtlich verantwortlich sind die dateneingebenden Behörden; sie tragen die Verantwortung für die Legalität der Datenerhebung und -speicherung sowie für die Richtigkeit und Aktualität der Daten. Nur sie dürfen Daten ändern, korrigieren, sperren oder löschen. Hat eine abfragende Stelle Zweifel an der Richtigkeit der Daten, hat sie dies umgehend mitzuteilen (§ 8 ATDG). Das BKA hat für die technische Protokollierung bei jedem Zugriff den Zeitpunkt, die abfragende Behörde, den Zugriffszweck und die Angaben, die die Feststellung der aufgerufenen Datensätze ermöglichen, zu garantieren, damit spätere Datenschutzkontrollen durch den Bundesdatenschutzbeauftragten beziehungsweise die Landesdatenschutzbeauftragten möglich sind. Allerdings sind die Protokolldaten nach 18 Monaten zu löschen (§§ 9 und 10 Abs. 1 ATDG).

Nach § 10 Abs. 2 ist das BKA „im Einvernehmen" mit der dateneingebenden Behörde in der Regel verpflichtet, Betroffenen Auskunft über zu ihnen gespeicherten Daten zu geben. Ausnahme hiervon sind Daten, die nach § 4 Abs. 1 ATDG im Sinne besonderer Geheimhaltungsinteressen „verdeckt gespeichert" wurden. In diesen Fällen richtet sich das Auskunftsersuchen direkt an die speichernden Behörden. Unrichtige oder unzulässigerweise gespeicherte Daten sind zu korrigieren beziehungsweise zu löschen. Ansonsten sind Daten

28 ebda., Rn. 71.

dann zu löschen, „wenn ihre Kenntnis zur Aufklärung oder Bekämpfung des internationalen Terrorismus nicht mehr erforderlich ist"; spätestens entsprechend der für die beteiligten Behörden geltenden Rechtsvorschriften (§ 11 Abs. 2 ATDG).

Nach § 12 ATDG legt das BKA die Details zur Errichtung der Antiterrordatei, wie zum Beispiel die „Bereiche des erfassten internationalen Terrorismus", die „weiteren beteiligten Polizeivollzugsbehörden" oder die Art und Eingabe der zu speichernden Daten, im Einvernehmen mit den beteiligten Behörden und mit Zustimmung des BMI, des Kanzleramtes, des Verteidigungsministeriums, des Bundesfinanzministeriums und der zuständigen obersten Landesbehörden in einer Errichtungsanordnung fest. Hierzu ist der Bundesdatenschutzbeauftragte anzuhören. Allerdings ist die Errichtungsanordnung als „Verschlusssache – Nur für den Dienstgebrauch" klassifiziert und daher nicht öffentlich zugänglich.

5 Nutzung und Kontrolle in der Praxis

Seit ihrer vollständigen Befüllung ab 2008, so berichtet die Bundesregierung 2013 von der unter Federführung des Bundesinnenministeriums durchgeführten Evaluierung des Antiterrordateigesetzes, waren in der ATD „annähernd konstant rund 18 000 Personen erfasst".[29] Davon sollen im August 2011 etwa 38 Prozent als Mitglieder oder Unterstützer einer „terroristischen Vereinigung" nach § 2 Satz 1 Nr. 1a ATDG gespeichert gewesen sein, 37 Prozent waren nach § 2 Satz 1 Nr. 2 als Anwender, Unterstützer, Vorbereiter, Befürworter und Hervorrufende „rechtswidrig(er) politischer Gewalt als Mittel zur Durchsetzung international ausgerichteter politischer und religiöser Belange" nach § 2 Satz Nr. 2 ATDG gespeichert . 19 Prozent zählten als Kontaktpersonen und sieben Prozent als Unterstützer der Unterstützer.[30] Für August 2012 berichtet das Bundesverfassungsgericht, dass nach Angaben der Bundesregierung fast 90 Prozent der von einer Speicherung betroffenen Menschen im Ausland lebe: nur 2.888 von 16.180 der zu diesem Zeitpunkt gespeicherten Datensätzen bezog sich auf im Inland lebende Personen.[31]

Nach Angaben des Evaluierungsberichts stammten etwa zwei Drittel der Datensätze von den Geheimdiensten, allein 46 Prozent vom Bundesnachrichtendienst und 15 Prozent vom Bundesamt für Verfassungsschutz (BfV).[32] Weitere 20 Prozent habe das BKA geliefert, zehn Prozent kämen von den Landeskriminalämtern. Marginal sei dagegen die Datenspeicherung durch Bundespolizei, MAD und ZKA, die jeweils weniger als 100 Datensätze einstellten. Von den Möglichkeiten der beschränkten oder verdeckten Speicherung werde relativ wenig Gebrauch gemacht, so unter anderem die Angaben von auskunftswilligen 160 Nutzerinnen und Nutzer aus den mehr als 60 beteiligten Behörden. Am ehesten werde die Option der verdeckten Speicherung durch das Bundesamt für Verfassungsschutz genutzt, das knapp ein Drittel der eingestellten Daten verdeckt speichere. [33] 2011 seien bei 44 Prozent der Personendatensätze erweiterte Grunddaten gespeichert gewesen, allerdings macht die Evaluation keine vollständigen Angaben, wie häufig welche Zusatzinformationen gespeichert sind.[34]

Profitiert von der ATD hat laut Evaluation insbesondere der polizeiliche Staatsschutz: Von den 232.447 Suchanfragen nach Personen, die zwischen 2007 und 2011 gestellt wurden, stammten 29 Prozent vom BKA und 55 Prozent von den Landeskriminalämtern; das geheimdienstliche Interesse war noch am größten bei den Landesämtern für Verfassungsschutz, die für knapp 10 Prozent der Suche verantwortlich waren.[35] Mehr als 1,4 Millionen Treffer habe es zwischen 2007 und 2011 gegeben, das heißt im Mittel wirft eine Suche sechs Treffer aus. Allerdings bleibt unklar, wie oft es sich dabei um die Ergebnisse einer gezielten Suche nach Personen oder von Inverssuchen handelt.

Nur selten werde die Möglichkeit genutzt, sich den Zugriff auf die erweiterten Grunddaten freischalten zu lassen. In der Regel scheint die an einen Treffer anschließende Kontaktaufnahme zum Beispiel telefonisch außerhalb der ATD zu erfolgen, so dass weitergehende Informationen dann auch außerhalb der ATD ausgetauscht würden. Dieser Kontakt auf „etablierten und bewährten Wegen der jeweils einschlägigen Rechtsvorschriften", so heißt es in der Evaluation, konnte durch die ATD intensiviert werden.

29 Deutscher Bundestag: Drucksache 17/12665 vom 07.03.2013, S. 5.
30 ebda., S. 32.
31 BVerfG, 1 BvR 1215/07 v. 24.4.2013, Rn. 68.
32 Deutscher Bundestag: Drucksache 17/12665 vom 07.03.2013, S. 5.
33 ebda., S. 34.
34 ebda., S. 38.
35 ebda., S. 43f.

Die Aktivierung der Ausnahmeregel „Eilfall", so die Bundesregierung gegenüber dem Bundesverfassungsgericht, habe es bislang nur einmal gegeben: Ein Landeskriminalamt habe direkt auf die erweiterten Grunddaten eines Datensatzes des Bundesamtes für Verfassungsschutz zugegriffen.[36] Diese Aussage überrascht insofern, als die Bundesregierung in ihrer Antwort auf eine Kleine Anfrage der Fraktion Bündnis 90/Die Grünen aus dem Jahr 2008 zumindest einen zweiten Fall schildert: Demnach soll von den Polizeibehörden des Bundes das BKA damals bislang einmal von der Eilfallregelung Gebrauch gemacht haben.[37]

Aufgrund der erleichterten Informationsanbahnung durch die Datei, aber auch durch das gemeinsame Arbeiten im GTAZ sei es „zu länder- und behördenübergreifenden Netzwerken aufgrund persönlicher Kontakte" gekommen. Mit der Datei, so schlussfolgert der Evaluierungsbericht, sei „die Kooperationsbereitschaft und das gegenseitige Vertrauen darauf, dass die jeweils vorhandenen Informationen vollständig zur Verfügung gestellt sind, ausgebaut und intensiviert" worden.[38] Tatsächliche Anhaltspunkte „für Folgewirkungen durch die Nutzung im Sinne von überschießend grundrechtsintensiven Eingriffen" hätten sich im Rahmen der Evaluation nicht ergeben.[39] Verwiesen wird unter anderem darauf, dass es im gesamten Evaluationszeitraum nur neun Anfragen von Personen beim BKA auf Auskunftsersuchen gegeben habe, wobei nur in einem Fall eine tatsächliche Speicherung in der ATD vorgelegen habe.[40] Ob die 90 Prozent der Betroffenen, die im Ausland leben, hinreichend Kenntnis über ihre entsprechenden Rechten haben, wird allerdings nicht thematisiert.

Aus den Stellungnahmen, die die Datenschutzbeauftragten im Verlauf des Verfahrens vor dem Bundesverfassungsgericht gemacht haben, geht hervor, dass von den 38 im Gesetz genannte Behörden bis zum Herbst 2012 nur die Hälfte überhaupt von Datenschützern kontrolliert worden war. Keine Kontrollbesuche gab es zum Beispiel bei den Landeskriminalämtern und Verfassungsschutzbehörden in den Bundesländern Nordrhein-Westfalen, Niedersachen oder Hessen. In Ländern, in denen Kontrollen stattgefunden hatten, waren diese überwiegend nur in der Startphase der Datei in den Jahren 2007/2008 erfolgt. Dabei waren zum Teil deutliche Probleme festgestellt worden hinsichtlich der Rechtmäßigkeit der Speicherung von Daten insbesondere von Kontaktpersonen. Kritisiert wurden aber auch grundlegende Kontrolllücken; so wurde zum Beispiel Mitarbeitenden von Datenschutzbeauftragten, obwohl diese sicherheitsüberprüft sind, mit Hinweis auf die „Staatswohlklausel" des Bundesdatenschutzgesetzes der Zugriff auf verdeckt gespeicherte Daten verweigert. Auch sei teilweise der elektronische Zugang zu Daten des Protokolldatenservers verweigert worden. Stattdessen seien den Kontrolleuren Papierausdrucke der Protokolle ausgehändigt worden, die sich einer schnellen computergestützten Auswertung entziehen.

6 Das Urteil des Verfassungsgerichts

In seiner Verfassungsbeschwerde gegen das Antiterrorgesetz von 2007 rügte der Beschwerdeführer eine Verletzung seiner Grundrechte auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. GG) auf das Brief- und Telekommunikationsgeheimnis (Art. 10 GG) auf Unverletzlichkeit der Wohnung (Art. 13 GG) sowie auf das Beschreiten des Rechtsweges gegen Akte der öffentlichen Verwaltung (Art. 19 Abs. 4 GG). Dabei wandte er sich insbesondere gegen Bestimmungen des Gesetzes zum Inhalt der Datei (§ 2 Satz 1 Nr. 2 und Nr. 3 ATDG), zu den zu speichernden Datenarten (§ 3 Abs. 1 Nr. 1 a und b sowie Abs. 2 ATDG) und zum direkten Zugriff abfragender Behörden auf die erweiterten Grunddaten im Rahmen der Eilfallregelung (§ 5 Abs. 2 ATDG).

6.1 Ausnahme vom grundrechtlichen Trennungsprinzip

Zentraler Maßstab der Prüfung des ATDG durch das Gericht ist das Recht auf informationelle Selbstbestimmung, dessen Schutzbereich durch die Zusammenführung und Neuanordnung von Daten aus verschiedenen Quellen sowie ihre Recherchierbarkeit durch andere als die ursprünglich datenerhebenden Stellen berührt werde. Im Rahmen seiner Verhältnismäßigkeitsprüfung kommt das Gericht zu dem Urteil[41], dass die ATD in ihren „Grundstrukturen" nicht zu beanstanden sei.

36 BVerfG, 1 BvR 1215/07 v. 24.04.2013, Rn. 71.
37 Deutscher Bundestag: Drucksache 16/10007 vom 18.07.2008, S. 8.
38 Deutscher Bundestag: Drucksache 17/12665 vom 07.03.2013, S. 48.
39 ebda., S. 51.
40 ebda., S. 52.
41 BVerfG, 1 BvR 1215/07 v. 24.04.2013.

Hierbei geht es von der Prämisse aus, dass die ATD „Vorinformationen vermitteln" will, „mit denen die Behörden schneller und zielführender Informationsersuchen bei anderen Behörden stellen können und die in dringenden Fällen auch eine erste handlungsleitende Gefahreneinschätzung ermöglichen".[42] Dieses Ziel einer schnellen Informationsanbahnung sei legitim und das ATDG zu seiner Erreichung geeignet und erforderlich, da Alternativen fehlten. Auch im engeren Sinne stehe die gesetzgeberische Grundrechtsbeschränkung nicht außer Verhältnis, da dem erheblichen Eingriffsgewicht durch den Informationsaustausch insbesondere zwischen Polizei und Nachrichtendiensten gewichtige öffentliche Belange gegenüberstünden, nämlich die effektive Aufklärung und Bekämpfung des internationalen Terrorismus und die Garantie eines zielführenden Austauschs der Erkenntnisse von Sicherheitsbehörden in einem föderalen Staat.

Aufgrund der sehr unterschiedlichen Aufgaben und Befugnisse von Geheimdiensten und Polizei leitet das Gericht erstmals explizit ein grundsätzliches „informationelles Trennungsprinzip" aus dem Grundrecht auf informationelle Selbstbestimmung ab: „Eine Geheimpolizei ist nicht vorgesehen."[43] Daten dürften zwischen den Diensten und der Polizei nur in Ausnahmefällen ausgetauscht werden. Insbesondere der Datenaustausch zur „operativen Aufgabenwahrnehmung" stelle einen besonders schweren Grundrechtseingriff dar, der nur einem „herausragenden öffentlichen Interesse" dienen dürfe und durch entsprechend hohe Eingriffsschwellen zu begrenzen sei.[44]

Der Grundrechtseingriff durch die auf Dauer angelegte Infrastruktur für den Informationsaustausch zwischen Geheimdiensten und Polizei werde aber dadurch gemindert, dass die Informationen – mit Ausnahme von Eilfällen nach § 5 Abs. 2 – „nicht unmittelbar zur Aufgabenwahrnehmung, insbesondere nicht zu operativen Zwecken" bereitgestellt würden, sondern als Grundlage für weitere Datenübermittlungen nur einen Informationsaustausch auf Grundlage des einschlägigen Fachrechts vorbereite.[45] Aus dem Verweis auf die fachrechtlichen Übermittlungsvorschriften ziehe das ATDG seine rechtsstaatlichen Grenzen. Entsprechend müssten diese allerdings „ihrerseits den verfassungsrechtlichen Anforderungen genügen". Dass das immer der Fall ist, stellt das Gericht allerdings deutlich in Frage, wenn es notiert, dass sich die Vorschriften für die Datenübermittlung zwischen Diensten und Polizei „nicht mit vergleichbar niederschwelligen Voraussetzungen wie der Erforderlichkeit für die Aufgabenwahrnehmung oder der Wahrung der öffentlichen Sicherheit"[46] begnügen könnten – ein impliziter, aber zentraler Verweis insbesondere auf die Regelungen zur fakultativen Spontanübermittlung aus §§ 18 und 19 des Bundesverfassungsschutzgesetzes (BVerfSchG), das jedoch nicht Gegenstand der Entscheidung war.

Regelungen zur fakultativen Spontanübermittlung aus dem Bundesverfassungsschutzgesetz

Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz (BVerfSchG) vom 20.12.1990, zuletzt geändert am 20.08.2012

§ 18 Abs. 2
Die Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, die Polizeien, die Behörden des Zollfahndungsdienstes sowie andere Zolldienststellen, soweit diese Aufgaben nach dem Bundespolizeigesetz wahrnehmen, und der Bundesnachrichtendienst dürfen von sich aus dem Bundesamt für Verfassungsschutz oder der Verfassungsschutzbehörde des Landes auch alle anderen ihnen bekanntgewordenen Informationen einschließlich personenbezogener Daten über Bestrebungen nach § 3 Abs. 1 übermitteln, wenn tatsächliche Anhaltspunkte dafür bestehen, daß die Übermittlung für die Erfüllung der Aufgaben der Verfassungsschutzbehörde erforderlich ist. Absatz 1 Satz 3 findet Anwendung.

§ 19 Abs. 1
Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an inländische öffentliche Stellen übermitteln, wenn dies zur Erfüllung seiner Aufgaben erforderlich ist oder der Empfänger die Daten zum Schutz der freiheitlichen demokratischen Grundordnung oder sonst für Zwecke der öffentlichen Sicherheit benötigt. Der Empfänger darf die übermittelten Daten, soweit gesetzlich nichts anderes bestimmt ist, nur zu dem Zweck verwenden, zu dem sie ihm übermittelt wurden.

Als „vorgelagerter Bestandteil dieses fachgesetzlichen Austausches"[47] verleihe die ATD den Einzelübermitt-

42 ebda., Rn. 106.
43 ebda., Rn. 122.
44 ebda., Rn. 123.
45 ebda., Rn. 125.
46 ebda., Rn. 126.
47 ebda., Rn. 127.

lungsvorschriften ein verändertes Gewicht. Es stelle sie in ein „vorinformiertes Umfeld" und ermögliche den andernfalls unmöglichen Austausch von Erkenntnissen. In der Folge erhöhe die ATD die Wahrscheinlichkeit, dass gespeicherte Personen aufgrund einer Abfrage von Informationen, die möglichweise auf bloßen Prognosen und subjektiven Einschätzungen der Behörden beruhen, unvermutet und ohne Chance zur Gegenwehr dem Umfeld des Terrorismus zugerechnet werden – mit eventuell beträchtlichen Konsequenzen.[48]

Obwohl das Gericht bei seiner Verhältnismäßigkeitsprüfung letztlich zu dem Ergebnis kommt, dass Gesetz und Datei aufgrund der Rücksichtslosigkeit des internationalen Terrorismus grundsätzlich verfassungsmäßig seien, formuliert es Nachforderungen an die Ausgestaltung des Informationsaustausches im Detail. Diese müsse, um den verfassungsrechtlichen Anforderungen zu genügen, hinreichend bestimmt sein und das Übermaßverbot respektieren.[49]

6.2 Klarstellung der beteiligten Behörden

Dass der volle Umfang der an der ATD beteiligten Behörden nur durch eine Errichtungsanordnung geregelt wird, die zudem als „Verschlusssache – Nur für den Dienstgebrauch" eingestuft ist, bemängelte das Gericht als unvereinbar mit dem Bestimmtheitsgebot. Die Regelung über den Kreis der Daten einstellenden und lesenden Behörden bilde den „Kern des spezifischen grundrechtlichen Gefährdungspotenzials"[50] der Antiterrordatei und bedürfe daher einer hinreichend klaren Bestimmung. Hingegen umschreibe § 1 Abs. 2 ATDG die beteiligten Behörden nur nach „weiten und wertungsoffenen Kriterien" und öffne damit die Bestimmung der Beteiligten „letztlich für allgemeine sicherheitspolitische Opportunitätserwägungen".[51] Stattdessen müsse die bisherige Verwaltungsvorschrift durch Außenrecht ersetzt werden, dass für die Rechtsunterworfenen und gegebenenfalls die Gerichte verbindlich sei. Ob der Kreis der beteiligten Behörden unmittelbar durch eine entsprechende Novellierung des ATDG oder aufgrund eines Gesetzes durch eine Rechtsverordnung bestimmt und die Entscheidung damit an die Exekutive delegiert wird, überlässt das Gericht allerdings dem Gesetzgeber.

6.3 Einschränkung des erfassten Personenkreises

Auch die Regelungen zum erfassten Personenkreis durch § 2 ATDG seien nicht in jeder Hinsicht mit dem verfassungsrechtlichen Anforderungen vereinbar.

Akzeptabel ist für das Gericht die Erfassung von Daten zu Personen, „die möglicherweise einer terroristischen Vereinigung angehören und sie unterstützen" nach § 2 Satz 1 Nr. 1 a und teilweise Nr. 1 b ATDG. Allerdings räumt das Gericht ein, dass die Vorschrift „beträchtlichen Raum für subjektive Einschätzungen der Behörden und ein weites Feld von Unwägbarkeiten" öffne, da die Norm an § 129 a StGB anknüpfe, der „strafbares Handeln schon weit in das Vorfeld von Rechtsverletzungen" vorverlagere. Gleichwohl hält es die Ausgestaltung für hinnehmbar, da im Rahmen die von der ATD intendierte Informationsanbahnung auch die Prüfung „ungesicherte[r] Einschätzungen von Verdachts- und Gefahrenlagen noch im Vorfeld von Ermittlungen" ermöglichen solle. Durch eine „sachgerechte Auslegung" der Tatbestandsmerkmale müsse sichergestellt werden, „dass eine Speicherung nicht auf bloßen Spekulationen beruhen darf". Zu gewährleisten sei dies durch die Rückbindung „tatsächlicher Anhaltspunkte" an „konkrete Erkenntnisse".[52]

Die pauschale Erweiterung des zu erfassenden Personenkreises um die Unterstützer von Unterstützern terroristischer Vereinigungen durch § 2 Satz 1 Nr. 1 b verstoße aber gegen den Grundsatz der Normenklarheit und das Übermaßverbot. Es dürfe nicht sein, dass Personen, die „weit im Vorfeld und möglicherweise ohne Wissen von einem Terrorismusbezug" arglos Organisationen, wie zum Beispiel „den Kindergarten eines Moscheevereins", unterstützten, in der ATD gespeichert würden. Allerdings räumt das Gericht dem Gesetzgeber die Möglichkeit ein, eine willentliche „Förderung der den Terrorismus unterstützenden Aktivitäten" zum Kriterium der Erfassung zu machen, wenn die Vorschrift hinreichend normenklar formuliert ist (Rn 149).

Umstritten war im Ersten Senat die Verfassungsmäßigkeit der Speicherung von Personen nach § 2 Satz 1 Nr. 2, in deren Zentrum der mehrdeutige Begriff der „rechtswidrigen Gewalt" steht, der im Kontext der Rechtsprechung zum Nötigungstatbestand („Zweite-Reihe-Rechtsprechung") bereits die Teilnahme an Blo-

48 ebda., Rn. 128.
49 ebda., Rn. 132ff.
50 ebda., Rn. 141.
51 ebda., Rn. 143.
52 ebda., Rn. 146.

ckadeaktionen meint.[53] Vier Mitglieder des Senats vertrauen aber auf die Auskunft der Sicherheitsbehörden, dass der Begriff in der Praxis der ATD enger verstanden würde und nur Gewalt meine, die „unmittelbar gegen Leib und Leben gerichtet oder durch den Einsatz gemeingefährlicher Mittel geprägt" sei.[54] Die Verhältnismäßigkeit sehen diese vier Senatsmitglieder auch gewahrt, wenn der Tatbestand des vorsätzlichen Hervorrufens „rechtswidriger Gewalt" eng – im Sinne eines willentlichen Hervorrufens – ausgelegt werde. Die vier anderen Senatsmitglieder sehen hingegen die Gefahr, dass die begriffliche Mehrdeutigkeit „aus Sicht der Sicherheitsbehörden auch sinnvoll und attraktiv erscheinen" könne, da sie es erlaube „einen nochmals wesentlich weiteren Kreis von Personen [...] vom Anwendungsbereich der Datei umfasst anzusehen".[55] Entsprechend würdigen sie einen an internationale Bestimmungen zur Terrorismusbekämpfung angelehnten Gegenvorschlag zur Einhegung des Gewaltbegriffs, der während des Gesetzgebungsverfahrens gemacht worden war. Einig war der Senat sich allerdings in der Ablehnung des Merkmals des Befürwortens von Gewalt, da dies auf eine „innere Haltung" abstelle. Auch wenn das Beispiel der öffentlich zu Hass und Gewalt anstachelnden „Hassprediger" in der ursprünglichen Begründung des Gesetzes genannt werde, greife der Wortlaut des Gesetzes auf einen „unverfügbaren Innenbereich des Individuums" zu und sei „in besonderer Weise geeignet, einschüchternde Wirkung auch für die Wahrnehmung der Freiheitsrechte" zu entfalten.[56]

Für verfassungswidrig erklärte das Gericht auch die Einbeziehung von Kontaktpersonen, die in der Formulierung von § 2 Satz 1 Nr. 3 ATDG prinzipiell das gesamte private und berufliche Lebensumfeld der Personen umfassen könne, die im eigentlichen Fokus der Datei stünden. Allerdings sei es verfassungsrechtlich nicht ausgeschlossen, auch Daten von Kontaktpersonen in der Datei zu erfassen. Nur seien Kontaktpersonen nach dem Zweck der Datei nur dann von Interesse, wenn sie „Aufschluss über die als terrorismusnah geltende Hauptperson vermitteln" könnten.[57] Für möglich halten die Richter und Richterinnen daher die verdeckt recherchierbare Speicherung von Kontaktpersonen mit wenigen Elementardaten, so dass eine Suche nach Hauptpersonen oder nach dem Klarnamen einer Kontaktperson nur zu einem Nachweis der informationsführenden Behörde samt Aktenzeichen führe.

Zusammengefasst verengt das Verfassungsgericht den Kreis der Personen, die in der ATD erfasst werden könnten, auf: 1) Angehörige und Unterstützer des internationalen Terrorismus mit Bezug zu Deutschland, 2) willentliche Förderer von Aktivitäten, die solchen Terrorismus unterstützen, 3) Personen, die „rechtswidrige Gewalt" – so der Begriff eng ausgelegt wird – als Mittel zur Durchsetzung international ausgerichteter politischer oder religiöser Belange anwenden, vorbereiten, unterstützen oder willentlich hervorrufen, sowie 4) Kontaktpersonen, wenn sie verdeckt recherchierbar gespeichert würden.

6.4 Dokumentationspflichten zur Kategorisierung von Informationen

Nicht beanstandet wird der Umfang der erfassten Daten. Allerdings betont das Gericht zum einen, dass selbst die Aussagekraft der Grunddaten durchaus erheblich sei, weil „höchstpersönliche Eigenheiten"[58] erfassten würden. Die Kombination der erweiterten Grunddaten zu einer Person nennt es gar einen „verdichteten Steckbrief".[59] Zum anderen anerkennt es, dass „die Speicherung im Ergebnis zu einem großen Teil auch Personen betreffen [dürfte], bei denen sich letztlich herausstellen wird, dass sie mit dem Terrorismus nichts zu tun haben".[60] Dennoch sei eine solche „Vorverlagerung der Terrorismusbekämpfung durch die Zusammenfügung"[61] der Daten – beschränkt auf „möglicherweise terrorismusnahe Personen" – rechtsstaatlich nicht ausgeschlossen angesichts der „eminenten Gefahren terroristischer Straftaten".[62]

Ergänzende Regelungen mahnt das Gericht aber an zur Klarstellung, wie die Merkmale Volkszugehörigkeit, Religionszugehörigkeit, terrorismusrelevante Fähigkeiten, Tätigkeiten in lebenswichtigen Einrichtungen sowie besuchte Orte und Gebiete in der Datei gespeichert werden. Da die Erfassung dieser relativ unbestimmten Merkmale in den erweiterten Grunddaten

53 vgl. zum Beispiel: BVerfG: Urteil vom 07.03.2011, Aktenzeichen BvR 388/05.
54 BVerfG, 1 BvR 1215/07 v. 24.04.2013, Rn. 151.
55 ebda., Rn. 154.
56 ebda., Rn. 161.
57 ebda., Rn. 165.
58 ebda., Rn. 168.
59 ebda., Rn. 174.
60 ebda., Rn. 169.
61 ebda., Rn. 169.
62 ebda., Rn. 175.

den „Zwischenschritt einer abstrakt-generellen Konkretisierung“[63] durch die Verwaltung bedürfe, müssten die Grundlagen entsprechender Entscheidungen durch eine verlässliche Dokumentation und Veröffentlichung nachvollziehbar und transparent gemacht werden. Das bisherige als „Verschlusssache – Nur für den Dienstgebrauch“ klassifizierte „Katalogmanual“, das – vereinfacht gesagt – die „Pull-Down Menüs“ definiert, die Nutzerinnen und Nutzern für die standardisierte Speicherung zum Beispiel des Merkmals „Volkszugehörigkeiten“ angeboten werden, reicht nach Ansicht des Gerichts jedenfalls nicht aus.

6.5 Begrenzung der Recherchemöglichkeiten

Die Regelungen zu Abfrage und Nutzung der Daten nach §§ 5 und 6 ATDG hält das Gericht weitgehend für verfassungsrechtlich unbedenklich. § 5 ATDG begrenze Abfragen und Recherchen, so stellt das Gericht klar, lediglich auf Einzelabfragen. Weder seien „Rasterung, Sammelabfragen oder eine übergreifende Ermittlung von Zusammenhängen zwischen Personen durch Verknüpfung von Datenfeldern“ erlaubt noch die Nutzung zu einer „automatischen Bilderkennung noch zur Verwendung von Ähnlichenfunktionen oder zur Abfrage mit unvollständigen Daten (so genannten ‚wildcards‘)“.[64] Eine weitere Nutzung der Daten jenseits der durch das ATDG normierten Informationsanbahnung ist nicht ausgeschlossen, bedarf aber laut Gericht eines weiteren Schritts nach Maßgabe des Fachrechts, das in der Verfassungsbeschwerde nicht zur Disposition stand und entsprechend im Urteil nur am Rande thematisiert wird.

Das Gericht stört sich allerdings an den Möglichkeiten zur blinden Recherche in den erweiterten Grunddaten. Zwar erlaubt es entsprechende namenbezogene Recherchen, die zum Beispiel die Identifizierung anderer Hauptpersonen ermöglichten, wenn mit dem Namen einer Kontaktperson gesucht würde. Für verfassungswidrig hält es aber die sogenannte Inverssuche nach anderen Merkmalen. Damit schließt es die Möglichkeit aus, zum Beispiel über die Suche nach einer Moschee die Klarnamen der Personen aus dem Datenbestand zu filtern, die dort verkehren. Vielmehr dürfe die Regelung nur so ausgestaltet sein, dass nicht mehr als Aktenzeichen und informationsführende Behörde angezeigt würden.[65]

6.6 Regelmäßige wirksame Kontrollen und Berichtspflichten

Angesichts der sehr begrenzten Auskunftsrechte und der entsprechend eingeschränkten Rechtsschutzmöglichkeiten für Betroffene, stellt das Gericht fest, dass die Kontrolle der Anwendung des ATDG im Wesentlichen bei der Aufsicht durch die Datenschutzbeauftragten liege. Damit erkennt es an, dass eine subjektivrechtliche Kontrolle teilweise nur mit beträchtlichem Verfahrensaufwand oder aufgrund von behördlichen Geheimhaltungsinteressen gar nicht realisierbar ist. Andererseits hält es die Einführung von nachträglichen Benachrichtigungspflichten oder eines Richtervorbehalts für nicht praktikabel oder sinnvoll. Entsprechende Bedeutung habe daher die effektive Kontrolle durch die Bundes- und Landesdatenschutzbeauftragten. Zudem müsse die Kontrolle regelmäßig erfolgen, zum Beispiel alle zwei Jahre, wie das Gericht anregt. Bei der Gewährleistung einer wirksamen aufsichtlichen Kontrolle sieht das Gericht sowohl den Gesetzgeber als auch die Behörden in der Pflicht. Unmittelbar gesetzgeberischen Nachbesserungsbedarf sieht es nur hinsichtlich des Erfordernisses „turnusmäßig festgelegter Pflichtkontrollen“. Technisch und organisatorisch sei die vollständige Protokollierung von Zugriffen und Änderungen des ATD-Datenbestandes zu gewährleisten, und die Protokollserverdaten müssten den Datenschutzbeauftragten in „praktikabel auswertbarer Weise“ zur Verfügung gestellt werden. Außerdem müsste die Datenschutzkontrolle mit wirksamen Befugnissen ausgestattet sein und dürfte nicht aufgrund föderaler Zuständigkeitsunklarheiten oder dem Verweis auf konkurrierende Kontrollgremien wie die G10-Kommission in ihrer Arbeit behindert werden: „Wenn der Gesetzgeber eine informationelle Kooperation der Sicherheitsbehörden vorsieht, muss er auch die kontrollierende Kooperation zugunsten des Datenschutzes ermöglichen.“[66]

Um darüber hinaus eine öffentliche Diskussion über den im Rahmen der ATD erfolgenden Datenaustausch und dessen demokratische Überprüfung zu ermöglichen, bedürfe es regelmäßiger und „inhaltlich gehaltvoller“ Berichte durch das BKA.[67] Eine entsprechende Berichtspflicht sei gesetzlich zu regeln.

63 ebda., Rn. 172.
64 ebda., Rn. 194.
65 ebda., Rn. 200.
66 ebda., Rn. 216.
67 ebda., Rn. 222.

6.7 Schutz des Fernmeldegeheimnisses und der Unverletzlichkeit der Wohnung

Für unvereinbar mit dem Brief- und Fernmeldegeheimnis (Art. 10 Abs. 1 GG) sowie dem Grundrecht auf die Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG) erklärt das Gericht die „vollständige und unterschiedslose" Einbeziehung von Informationen, die etwa im Rahmen einer Telekommunikationsüberwachung oder eines Großen Lauschangriffs gewonnen wurden – und ergänzt, obwohl sie nicht vom Beschwerdeführer gerügt wurden, Eingriffe in das Grundrecht auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V. mit Art. 1 Abs. 1 GG) durch Online-Durchsuchungen.[68] Angesichts der Schwere der Grundrechtseingriffe durch diese Formen der verdeckten Datenerhebung sind die Anforderungen an Weitergabe und Zweckänderungen entsprechend gewonnener Informationen hoch. Es gilt, dass die strengen Eingriffsschwellen durch eine Datenweitergabe nicht unterlaufen werden dürfen, wozu die Informationen unter anderem zu kennzeichnen sind. Durch die Speicherung solcher Informationen in der ATD, auch wenn sie gekennzeichnet sind, sieht das Gericht nun die Gefahr, dass diese „einer großen Anzahl von Behörden ohne weiteres als Vorabinformationen zugänglich gemacht [... und] noch weit im Vorfeld greifbarer Gefahrenlagen zur Verfügung gestellt" werden könnten. Für verfassungskonform hält das Gericht eine Regelung, „ die für solche Daten stets eine verdeckte Speicherung gemäß § 4 ATDG", was bislang aber nicht klar normiert ist.[69]

6.8 Übergangsregelung bis Ende 2014

Überzeugt von der „Bedeutung der Datei für die Abwehr des internationalen Terrorismus" fürchtet das Gericht, dass eine unmittelbare Nichtigkeitserklärung der beanstandeten Normen „dem Schutz überragender Güter des Gemeinwohls die Grundlage" entziehen würde. Daher stellt es nur ihre Unvereinbarkeit mit dem Grundgesetz fest. Befristet bis zum 31. Dezember 2014 dürfen die verfassungswidrigen Vorschriften nun weiter angewendet werden, allerdings mit drei Einschränkungen: Außerhalb von Eilfällen gemäß § 5 Abs. 2 ATDG ist auszuschließen, erstens, der Zugriff auf die Daten von Kontaktpersonen, zweitens, der Zugriff auf Daten, die im Rahmen von Telekommunikations- oder Wohnraumüberwachungen gewonnen wurden, und drittens, bei Recherchen in den erweiterten Grunddaten der Zugriff auf die Grunddaten zu Personen.[70]

Durch die Einräumung einer „großzügige[n]" Frist will das Gericht dem Gesetzgeber die Möglichkeit nicht nur zur Novellierung des ATD einräumen, sondern auch von vergleichbaren Bestimmungen anderer Gesetze „sowie eventuell von Datenübermittlungsvorschriften einzelner Sicherheitsbehörden".

6.9 Verfassungsgerichtliche Mindestanforderungen an die Neufassung des Gesetzes

Zusammengefasst ergeben sich aus dem Urteil des Bundesverfassungsgerichts zur Beschwerde gegen das ATDG für den Gesetzgeber folgende Mindestanforderungen an die Novellierung des Gesetzes, das zur Verhandlung stand:

1 Normierung des Kreises der beteiligten Behörden durch die zwingende Vorschrift, eine abschließende Regelung per Rechtsverordnung zu erlassen, durch eine Änderung von §§ 1 Abs. 2 und 12; dabei muss das Gesetz klare Vorgaben für die Auswahl der Behörden machen.
2 Eingrenzung des zu erfassenden Personenkreises auf willentliche Förderer von Aktivitäten, die den Terrorismus unterstützen, durch eine Änderung von § 2 Satz 1 Nr. 1 b.
3 Streichung der Befürworter von „rechtswidriger Gewalt" aus dem nach § 2 Satz 1 Nr. 2 zu erfassenden Personenkreises .
4 Neuordnung der Speicherung der Daten aller Kontaktpersonen nach § 2 Satz 1 Nr. 3 durch ihre Zuordnung zu den erweiterten Grunddaten von Hauptpersonen nach dem Vorbild von § 3 Abs. 1 Nr. 1 b oo.
5 Ergänzung des ATDG um eine Bestimmung, die eine nachvollziehbare Dokumentation und Veröffentlichung der Kategorisierungsregeln (zum Beispiel in Form eines „Katalogmanuals") für die in nach § 3 Abs. 1 Nr. 1 b den erweiterten Grunddaten zu speichernden Angaben zu Volkszugehörigkeit (gg), Religionszugehörigkeit (hh), besondere terrorismusrelevante Fähigkeiten (ii), Tätigkeiten in einer lebenswichtigen Einrichtung (kk), besuchten Orte oder Gebieten (nn).
6 Verbot der merkmalsbezogenen Recherche („Inversuche") in den erweiterten Grunddaten durch eine

68 ebda., Rn. 226.
69 ebda., Rn. 228.
70 ebda., Rn. 229.

Begrenzung der Suchmöglichkeiten auf namensbezogene Recherchen durch eine entsprechende Präzisierung von § 5 Abs. 1 ATDG.

7 Ergänzung des ATDG um eine Vorschrift zu regelmäßigen und wirksamen Kontrollen der an der Verbunddatei beteiligten Behörden durch die Datenschutzbeauftragten von Bund und Ländern.

8 Ergänzung des ATDG um eine Verpflichtung des BKA zur regelmäßigen Veröffentlichung hinreichend gehaltvoller Berichte über den Betrieb und die Nutzung der ATD.

9 Normierung der verdeckten Speicherung von Daten, die durch Eingriffe in die Grundrechte auf das Telekommunikationsgeheimnis, die Unverletzlichkeit der Wohnung und die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme erhoben wurden, durch eine Änderung von § 13 ATDG.

7 Bewertung und Empfehlungen

Obwohl durch das Antiterrordateigesetz erstmals, seitdem die Datenverbindung zwischen BKA und Verfassungsschutz Anfang der 1990er Jahre unter dem Eindruck des Volkszählungsurteils gekappt worden war, wieder Informationen von Polizei und Diensten zusammengeführt werden, hat das Bundesverfassungsgericht die ATD nicht insgesamt für verfassungswidrig erklärt. Gleichwohl leitet es aus dem Recht auf informationelle Selbstbestimmung das Prinzip einer informationellen Trennung zwischen der zum Einsatz von Zwangsmitteln befugten Polizei und den im Geheimen operierenden Diensten ab, das nur in Ausnahmefällen und unter strikten Auflagen durchbrochen werden darf. Entsprechend verweist das Urteil an vielen Stellen auf die erheblichen Risiken einer Datei, die Informationen von Polizei und Geheimdiensten dauerhaft in einer technischen Infrastruktur bündelt. Für tolerabel hält das Gericht die Risiken der ATD nur im Schatten der Bedrohung, die es im internationalen Terrorismus sieht.

Damit setzt das Urteil einen deutlich anderen Akzent, als die Bund-Länder-Kommission Rechtsterrorismus, die in ihrem Abschlussbericht zur Verbesserung der Zusammenarbeit zwischen Polizei, Verfassungsschutz und Justiz schreibt: „Das Trennungsgebot beinhaltet jedoch kein Zusammenarbeitsverbot bzw. das Gebot einer informationellen Abschottung, sondern lässt im Rahmen der jeweiligen Aufgabenwahrnehmung einen Informationsaustausch zwischen Verfassungsschutz und Polizei zu. […] Ein informationelles Trennungsgebot widerspräche schließlich auch dem Sinn der Verfassungsschutzbehörden: Die Sammlung und Auswertung von Informationen darf kein Selbstzweck sein. Daher müssen die Verfassungsschutzbehörden ihre Daten an diejenigen Stellen weitergeben, die die erforderlichen Maßnahmen ergreifen können.“[71] Diese Aussagen können nach dem Urteil nicht mehr aufrechterhalten werden; in dieser Hinsicht kann der Bericht daher nicht zur Grundlage weiterer politischer Entscheidungen gemacht werden.

Die Prämissen, die das Gericht an einen verfassungskonformen Betrieb der ATD legt, sind höchst voraussetzungsvoll. So ist vielfach auf die „sachgerechte“ und enge Auslegung unbestimmter Rechtsbegriffe in der Praxis und die auch zukünftig der Lesart Karlsruhes folgende Anwendung von Einzelvorschriften zu vertrauen, zum Beispiel wenn es um die das Verständnis von „rechtswidriger Gewalt“ geht oder das Verbot von Sammelabfragen verlässlich befolgt werden soll. Angesichts der eingangs skizzierten Verschiebungen in der bundesdeutschen Sicherheitsarchitektur stellt sich die Frage, wie dies dauerhaft sichergestellt und überprüft werden kann. Zudem ist zu überlegen, ob und wie selbst bei einer entsprechend gestärkten Kontrolle durch die Datenschutzbehörden die Richtigkeit von Daten und die Zulässigkeit ihrer Speicherung überprüft werden kann, wenn diese in ihrer überwältigenden Mehrheit aus dem Ausland und von den geheim arbeitenden Nachrichtendiensten stammen. Auszuschließen ist insbesondere die Speicherung und Weiterverarbeitung von Informationen, die durch die Sicherheitsbehörden anderer Staaten unter Anwendung oder Androhung von Folter gewonnen wurden.

Die Minimalvariante einer Umsetzung der sich auf dem Urteil ergebenden Mindestanforderungen wird keine hinreichende Garantie für einen verfassungskonformen Betrieb der ATD bieten. Eine entsprechende Ausstattung der Datenschutzbehörden ist ebenso zu gewährleisten wie eine rigide und sanktionsbereite Dienst- und Fachaufsicht über die alltägliche Praxis der Nutzerinnen und Nutzer der ATD und ihre Kooperation mit den Aufsichtsbehörden. Eine gesetzliche Konturierung der unbestimmten, aber vom Verfassungsgericht nicht beanstandeten Rechtsbegriffe durch den Bundesgesetzgeber würde hier helfen; zu denken ist insbeson-

71 Bundesministerium des Innern und Ständige Konferenz der Innenminister und –senatoren der Länder (Hg.) (2013): Abschlussbericht der Bund-Länder-Kommission Rechtsterrorismus vom 30. April 2013, S. 32f.

dere an den Terminus „rechtswidrige Gewalt". Sinnvoll wäre ebenfalls eine eindeutige Klarstellung der Beschränkung der Nutzung auf Einzelabfragen. Zudem sollten angesichts der geänderten Vorzeichen die Pflicht zur Evaluierung erneuert und die Anforderungen an die Unabhängigkeit und den menschenrechtlichen Prüfmaßstab einer solchen Evaluierung gestärkt werden.[72]

Darüber hinaus stellt das Gericht die Datei aber in einen größeren Kontext, der in seinem Urteil nur wenig prominent aufscheint. Wenn der Erste Senat betont, dass auch die fachrechtlichen Übermittlungsvorschriften den verfassungsrechtlichen Vorgaben entsprechen müssen und dem Gesetzgeber nun insbesondere deshalb eine so großzügige Frist einräumt, damit er vergleichbare Vorschriften anderer Gesetze prüft und „eventuell" die Übermittlungsvorschriften einzelner Sicherheitsbehörden, ist dies ein unübersehbarer Hinweis für die Gesetzgeber. Zu denken ist nämlich nicht nur an das Rechtsextremismusdateigesetz, sondern auch und insbesondere an das Bundesverfassungsschutzgesetz. Mindestens dessen zentrale Datenübermittlungsvorschriften §§ 18 und 19 sowie vergleichbare Normen aus den Gesetzen über BND und MAD und aus den Landesverfassungsschutzgesetzen will Karlsruhe offensichtlich geprüft sehen.

Wer das informationelle Trennungsprinzip ernst nimmt, darf sich nicht damit begnügen, nur die Antiterrordatei als „vorgelagerten Bestandteil" des fachgesetzlichen Austausches einer Revision zu unterziehen. Vielmehr gilt es, den Kern in den Blick zu nehmen und zu prüfen, ob die Voraussetzungen für den Datenaustausch zwischen Nachrichtendiensten und Polizei in ihrer jetzigen Form bestehen bleiben können. Entsprechend darf es bei den Verhandlungen über die Harmonisierung der gesetzlichen Übermittlungsvorschriften von Bund und Ländern, die im Gefolge des Abschlussberichts der Bund-Länder-Kommission Rechtsterrorismus zu erwarten sind, nicht primär um die Beseitigung von „Schnittstellenproblemen" gehen. Vielmehr muss sichergestellt werden, dass die Voraussetzungen für den Datenaustausch nicht abgesenkt, sondern – orientiert am Maßstab des „herausragenden öffentlichen Interesses" – klar definiert und begrenzt werden. Entsprechend sind nicht nur die Regelungen für den fakultativen Datenaustausch auf den Prüfstand zu stellen; eine klare Absage zu erteilen ist auch den Vorschlägen der Bund-Länder-Kommission Rechtsterrorismus, die Übermittlungspflichten selbst auf Bereiche der „mittleren Kriminalität" auszuweiten, um zum Beispiel die Weitergabe des „Beifangs" zu Drogen- oder Eigentumsdelikten aus geheimdienstlichen Überwachungen an die Polizei zu erzwingen.[73]

Abschließend verwiesen sei daher auf die wichtige Feststellung des ehemaligen UN-Sonderberichterstatters für die Förderung und den Schutz der Menschenrechte in der Terrorismusbekämpfung, Martin Scheinin, der 2009 in einem Bericht zur Rolle der Nachrichtendienste schrieb:

„Eindeutige Rechtsgrundlagen für das Handeln der Nachrichtendienste helfen auch, ihre Aufgaben von denen der Polizei zu unterscheiden. Fehlt diese klare Unterscheidung führt dies zum Verschwimmen der Verantwortlichkeiten und damit zum Risiko, dass Sondervollmachen in Alltagssituationen zum Einsatz kommen, ohne dass eine überragende Gefahr für die Bevölkerung besteht."[74]

Scheinin verweist auf die Entscheidung des Europäischen Gerichtshofes für Menschenrechte im Fall Rotaru vs. Rumänien, dass geheimdienstliche Eingriffe in das Recht auf Privatsphäre (Artikel 8 der Europäischen Menschenrechtskonvention) nicht einfach nur einer Rechtsgrundlage bedürfen, sondern die „Qualität" entsprechender Gesetze hinsichtlich der Vorhersehbarkeit ihrer Konsequenzen entscheidend ist.[75] Genau dies ist der Kern des institutionellen Trennungsgebotes, den das Bundesverfassungsgericht aus den Grundrechten abgeleitet hat, und der Maßstab für die Überprüfungen, die nun notwendig sind.

72 Siehe hierzu: Weinzierl, Ruth (2006): Die Evaluierung von Sicherheitsgesetzen. Anregungen aus menschenrechtlicher Perspektive. Policy Paper No. 6. Berlin: Deutsches Institut für Menschenrechte; Albers, Marion / Ruth Weinzierl (Hg.) (2010): Menschenrechtliche Standards in der Sicherheitspolitik. Beiträge zur rechtsstaatsorientierten Evaluierung von Sicherheitsgesetzen. Baden-Baden: Nomos; Ziekow, Jan / Alfred G. Debus / Axel Piesker (2012): Leitfaden zur Durchführung von ex-post-Gesetzesevaluationen unter besonderer Berücksichtigung der datenschutzrechtlichen Folgen im Auftrag des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Speyer: Institut für Gesetzesfolgenabschätzung und Evaluation. http://www.bfdi.bund.de/SharedDocs/Publikationen/Allgemein/Evaluation_Leitfaden.pdf?__blob=publicationFile [abgerufen am 22. November 2012].

73 Bundesministerium des Innern und Ständige Konferenz der Innenminister und –senatoren der Länder (Hg.) (2013): Abschlussbericht der Bund-Länder-Kommission Rechtsterrorismus vom 30. April 2013, S. 239-245.

74 „Clear legislated powers for intelligence agencies also help to distinguish between the tasks of intelligence and law enforcement agencies. Failure to make these clear distinctions will lead to blurred lines of accountability and to the risk that special powers are used in routine situations where there is no pre-eminent threat to the population." - UN, Generalversammlung, UN Dok. A/HRC/10/3 vom 04.02.2009, Ziffer 31.

75 EGMR: Urteil vom 04.05.2000, Antragsnummer 28341/95, Ziffer 52.

Deutsches Institut für Menschenrechte

Zimmerstr. 26/27

10969 Berlin

Tel.: 030 25 93 59 - 0

Fax: 030 25 93 59 - 59

info@institut-fuer-menschenrechte.de